Apprécier les risques M 22

|  |  |
| --- | --- |
| type | processus de management |
| finalité | * atteindre les objectifs du SMSI * établir les critères de risque de sécurité de l’information * identifier, analyser et évaluer les risques de sécurité de l’information * améliorer la performance globale de l’entreprise |
| pilote | directeur / responsable sécurité de l’information / chef de projet |
| risques | * ne pas prendre en compte le contexte de l’entreprise * ne pas comprendre les exigences des parties intéressées * ne pas identifier les risques * ne pas analyser les risques * ne pas évaluer les risques * ne pas établir les critères d’acceptation des risques * ne pas tenir à jour les critères d’acceptation des risques * ne pas identifier les pilotes des risques * ne pas passer en revue les indicateurs |
| processus amont | * réaliser une AMDEC * planifier le SMSI |
| processus aval | * traiter les risques * piloter les processus * communiquer * satisfaire aux exigences |
| éléments d'entrée | * contexte de l’entreprise * exigences des parties intéressées * ressources nécessaires * conditions (normales et anormales) * tout risque identifié * achats informatiques |
| activités  (sous-processus) | * établir les critères d’acceptation des risques * identifier les risques * attribuer les risques à des pilotes * analyser les risques * évaluer les risques * sensibiliser le personnel sur les risques * communiquer * conserver les informations documentées sur l’appréciation des risques |
| éléments de sortie | * critères d’acceptation des risques * liste des risques * niveaux des risques * liste des pilotes de risque * sensibilisation du personnel |
| ressources | direction, responsables départements, pilotes processus, pilotes risques |
| indicateurs | * risques identifiés * risques évalués |
| procédures / documents | amélioration continue, communication, audits internes, formation, planification, gestion des changements, achats, maîtrise des processus, analyse des données, inspection / plan stratégique, politique, objectifs, indicateurs, liste des risques, plans d'action, liste processus, fiches processus, enquête de satisfaction clients, demandes de changement, rapports, AMDEC |
| clients | l’ensemble du personnel et des processus, parties intéressées |

Glossaire :

SMSI : système de management de la sécurité de l’information

AMDEC : analyse des modes de défaillance, de leurs effets et de leur criticité

directeur / responsable sécurité de l’information / chef de projet

* atteindre les objectifs du SMSI
* établir les critères de risque de sécurité de l’information
* identifier, analyser et évaluer les risques de sécurité de l’information
* améliorer la performance globale de l’entreprise

apprécier les risques /

M 22

titre / codification

finalité

pilote

processus aval

risques

processus amont

* traiter les risques
* piloter les processus
* communiquer
* satisfaire aux exigences
* réaliser une AMDEC
* planifier le SMSI
* ne pas prendre en compte le contexte de l’entreprise
* ne pas comprendre les exigences des parties intéressées
* ne pas identifier les risques
* ne pas analyser les risques
* ne pas évaluer les risques
* ne pas établir les critères d’acceptation des risques
* ne pas tenir à jour les critères d’acceptation des risques
* ne pas identifier les pilotes des risques
* ne pas passer en revue les indicateurs

éléments de sortie

activités

éléments d'entrée

* critères d’acceptation des risques
* liste des risques
* niveaux des risques
* liste des pilotes de risque
* sensibilisation du personnel
* contexte de l’entreprise
* exigences des parties intéressées
* ressources nécessaires
* conditions (normales et anormales)
* tout risque identifié
* achats informatiques
* établir les critères d’acceptation des risques
* identifier les risques
* attribuer les risques à des pilotes
* analyser les risques
* évaluer les risques
* sensibiliser le personnel sur les risques
* communiquer
* conserver les informations documentées sur l’appréciation des risques

clients

procédures / documents

indicateurs

ressources

l’ensemble du personnel et des processus, parties intéressées

amélioration continue, communication, audits internes, formation, planification, gestion des changements, achats, maîtrise des processus, analyse des données, inspection / plan stratégique, politique, objectifs, indicateurs, liste des risques, plans d'action, liste processus, fiches processus, enquête de satisfaction clients, demandes de changement, rapports, AMDEC

risques identifiés

risques évalués

direction, responsables départements, pilotes processus, pilotes risques